REMARKS/ARGUMENTS

Claims 1-11 are pending in this application. By this Amendment, claims 1, 2 and 6 are amended and claims 10-11 are new. The amendments introduce no new matter. The Office Action rejects claims 1-9 under 35 U.S.C. §101 as being directed to non-statutory subject matter. The Office Action also rejects claims 1-9 under 35 U.S.C. §103(a) as unpatentable over Matyas (U.S. Pat. 5,953,420) in view of Newcombe (U.S. Pub. 2003/0172269, now U.S. Patent 7,392,390). These rejections are respectfully traversed.

Interview Summary

Applicants thank Examiner Nigh for the courtesy extended to the undersigned representative during the interview conducted February 10, 2010. During the interview, the issue of whether a "ticket" as described in Newcombe is similar to a "token" as recited in the claims was discussed. Applicants' representative argued that one of ordinary skill in the art would understand the difference between the terms "token" and "ticket," and that the tickets in Newcombe could not reasonably be interpreted to be the tokens as recited in the claims because they are mere data structures and are not capable of performing the functions ascribed to a token, such as generating a one-time password and sending that one-time password to an authentication server. The Examiner argued that an alleged lack of a physical description of the "token" in the specification beyond that it is a "physical device" could require a broadest reasonable interpretation of the term to include the use of a data structure like the ticket disclosed in Newcombe. No agreement was reached.

The applicability of a 35 USC §112 rejection to the language in claims 2 and 6 related to the "if" statements was also discussed. Applicants' representative argued that this language complies with 35 USC §112 because one of skill in the art would readily understand the scope of each claim.

No other pertinent matters were discussed.

Rejections under 35 U.S.C. 101

Claims 1-9 stand rejected as directed to non-statutory subject matter. Applicants respectfully disagree with the analysis presented in the Office Action. However, solely to advance prosecution of the application, claim 1 is amended to recite, *inter alia*, that certain method steps are performed by a computer. Also, Claims 2 and 6 have been amended to state that certain method steps are performed by the authentication server. Applicants respectfully submit that the claim complies with the interpretation of §101 as applied by the Office Action. Withdrawal of the rejection is respectfully requested.

Rejection of Claim 1-9 under 35 U.S.C. 103(a)

To support a prima facie case of obviousness, the Examiner must demonstrate that each feature recited in the claims is found in the cited art, or provide explicit reasoning to support the finding that the features would be obvious to one of skill in the art at the time the invention was made. See M.P.E.P. §§ 2141, 2142. The Office Action asserts that each and every feature recited in the claim is shown by the cited references. Thus, to support the rejection of these claims, the Examiner must show where each feature recited in the claim is disclosed by one of the cited references.

The Office Action Fails to Show that the Cited References Disclose or Suggest a "Token."

Claim 1 recites, in relevant part:

> A method for calculating a One Time Password, comprising:
>
> where the secret is uniquely assigned to a token and is shared between the token and an authentication server; and
>
> the count is a number that increases monotonically at the token with the number of One Time Passwords generated by the token and increases monotonically at the authentication server with each calculation at the authentication server of a One Time Password;

Independent claims 2 and 6 also recite the use of a token. The Office Action admits that, "Matyas does not explicitly disclose a token." Office Action, p. 4. However, the Office Action asserts that , "Newcombe teaches a token and a method of assigning a secret to a ticket (similar to a token)." *Id* (emphasis added). Applicants respectfully disagree.

A "ticket" is not "similar to a token" as that term would be understood by one of ordinary skill in the art. A ticket is a mere passive data structure that is produced by another device (such as an authentication server). Once the ticket is produced, no further changes are made to that particular ticket. A token, on the other hand, is capable of performing some functionality including creating and sending passive data structures (such as the information that is carried on a ticket) that can be used to authenticate a user. Indeed, insofar as they may be used for similar purposes, a ticket is more like the data sent by the token rather than the token itself. The use of tokens is described at page 1, line 30 – page 2, line 10, page 2, lines 22-26, and throughout the specification as filed. Based on the present disclosure and the use of the term in the art, a person of ordinary skill in the art would not consider a ticket to be equivalent to a token as recited in the claims. Therefore, withdrawal of the rejection based on this rationale is respectfully requested.

Furthermore, even if the term "token" could be considered to include a "ticket," the tickets recited in Newcombe do not (and cannot) perform the functions of a token as recited in the claims. Newcombe is directed to an improved system and method for authenticating a client in a distributed environment using Kerberos style authenticators. Newcombe, Abstract; [0002]. Newcombe involves the use of three different types of servers: an Authentication Server, a Ticket-Granting-Server, and Content Servers. *Id.* at [0064]; [0068]. The Authentication Server, after it authenticates a client, issues a ticket-granting-ticket, which usually contains a server readable portion (i.e. encrypted so that only the Ticket-Granting-Server can read), a client readable portion (usually encrypted with the clients hash salted password), and a modified authenticator (including a timestamp, local IP address, and remote IP address). *Id.* at [0064]-[0065]. The ticket-granting-ticket is then delivered to the Ticket-Granting-Server, which utilizes the server readable portion of the ticket-granting-ticket (along with other information) to authenticate the user. *Id.* at [0068]. The ticket granting server then gives the client content tickets that permit the client to access the Content Servers. *Id.* at [0072]. The Content Servers

utilize the content tickets (along with other parameters) to authenticate the user and allow access to the specific content. *Id.*

The tickets described in Newcombe are simply messages containing encrypted information that are delivered to a client by either the Authentication Server or the Ticket-Granting-Server. Newcombe, [0064]-[0065]; [0068]. There is simply no disclosure that suggests that any of these "tickets" are capable of generating anything, let alone that a one time password is generated by the "ticket." Indeed, the ticket is already in its final form when the client receives it, and the ticket itself is passed along to the appropriate server to authenticate the client (the client cannot modify the server readable portion of any ticket because it is encrypted). *Id.* at [0065] ("tamper-proof server readable portion"); [0032] (describing how a ticket can be encrypted to protect the information on it). Therefore, a person of ordinary skill in the art would not interpret the use of "tickets" in Newcombe to disclose the use of a token as recited in claim 1.

This is further evidenced by Newcombe itself, which explicitly addresses tokens and the use of tokens in authentication systems:

> Once the software is downloaded, the user may share the downloaded software with a friend. Some Internet sites attempt to limit sharing of the software by requiring a user password, a Compact Disc (CD) key, token, or the like to be provided to the Internet server prior to obtaining access to the software. Typically, should a password, token, or key be shared or stolen, the unauthorized user would still be able to access the software. Therefore, there is a need in the industry for enabling improved authentication in a distributed environment. Thus, it is with respect to these considerations and others that the present invention has been made

Newcombe, [0004]. Newcombe thus distinguishes between a "token" and the "tickets" cited by the Office Action, and clearly indicates that the two are not equivalent. In fact, Newcombe states that a problem with using tokens is that if the token gets lost or stolen then an unauthorized individual could have continued access to the protected content. Therefore, it is not reasonable to suggest that the tickets described in Newcombe's system are similar to a token, as that term would be understood to one of ordinary skill in the art, when the alleged limitations of using tokens were one of the stated reasons that Newcombe implemented a system that utilizes tickets.

When interpreting a claim term, the "broadest reasonable interpretation" applied by the Office must be consistent with the use of the term in the specification. M.P.E.P. §2111. The present specification indicates that "tokens" are understood in the art to be devices used for authentication:

> A token is a device that can be used to authenticate a user. It can include one or more secrets, some of which can be shared with a validation center. For example, a token can store a secret key that can be used as the basis for calculating a One Time Password (OTP). A OTP can be a number (or alphanumeric string) that is generated once and then is not reused. The token can generate an OTP and send it along with a unique token serial number to an authentication server. . . . To further strengthen the link from the user to the token, the user can establish a Personal Identification Number (PIN) shared with the token that must be entered by the user to unlock the token. Alternatively, the PIN can be shared between the user, the token and the authentication server, and can be used with other factors to generate the OTP. A token typically implements tamper-resistant measures to protect the secrets from unauthorized disclosure.

[0004]. The use and configuration of tokens in the present invention is further described throughout the specification, and these features are provided only as non-limiting illustrations. Newcombe's tickets cannot properly be said to have any of these properties – they are mere data structures (*see* Newcombe, [0007]), not devices, and they are not capable of generating an OTP, being locked or unlocked with a PIN, or having tamper-proof measures that prevent disclosure of information contained within them. For at least this reason, the interpretation applied by the Office Action to the tickets in Newcombe is inconsistent with the use of the claim terms in the specification.

Therefore, the Office Action fails to support a *prima facie* case of obviousness with respect to claims 1,2 and 6. The rejection of dependent claims 3-5 and 7-9 is similarly unsupported by the Office Action, and these claims are allowable for at least the same reasons as the independent claims. For at least this reason, the rejection of claims 1-9 should be withdrawn.

The Office Action Fails to Show that the Cited References Disclose or Suggest that a Secret is Uniquely Assigned to a Token.

Claim 1 recites, in relevant part:

> A method for calculating a One Time Password, comprising:
>
> where the secret is uniquely assigned to a token and is shared between the token and an authentication server; and

Claims 10 and 11 recite similar features The Office Action admits that Matyas does not disclose, "where the secret is uniquely assigned to [a] token and is shared between the token and an authentication server," but asserts that Newcombe teaches, "a method of assigning a secret to a ticket (similar to a token). Office Action, p. 4. Applicants respectfully disagree.

Even assuming, *arguendo*, that a ticket in Newcombe and a token as recited in the claims are similar, Newcombe does not teach that the secret is uniquely assigned to a "ticket." (interpreted as the recited "token"). Applicant notes that the Office Action does not specifically mention what it considers to be the secret that is "uniquely assigned" to the ticket in Newcombe. However there is simply no information at all that is uniquely assigned to a ticket. The session key that is disclosed is used not only by the ticket-granting-ticket but also by the content tickets as well. Newcombe, [0065]; [0072]. Similarly, the information regarding the user (i.e. account and IP addresses) and life-time parameters all appear in other tickets. *Id.* at [0072]. Finally, the timestamp could hardly be considered "a secret," as one of ordinary skill in the art would understand that term. However, even if it was considered as such, Newcombe discloses that the content tickets also include the timestamps. *Id.* ("[C]ontent [S]erver may be configured to perform substantially the same mechanisms to authenticate the client, as described . . . for [the] [Ticket Granting Server]").

Thus, even if a ticket is similar to a token, Newcombe provides no disclosure or suggestion that a secret is uniquely assigned to a "ticket." The Office Action does not assert that the other cited reference discloses these features, nor is there any other suggestion in the record that the other reference remedies these deficiencies of Newcombe. Therefore, whether considered alone or in combination, the references as applied by the Office Action fail to support

a *prima facie* case of obviousness with respect to claims 1, 2 and 6. The rejection of dependent claims 3-5 and 7-9 is similarly unsupported by the Office Action, and these claims are allowable for at least the same reasons as the independent claims. For at least this reason, the rejection of claims 1-9 should be withdrawn.

Rejections of Claims 2-9 under 35 U.S.C. 103(a)

The Office Action Fails to Show that the Cited References Disclose or Suggest that if the Calculated One Time Password Does Not Correspond to the Received One Time Password, then Incrementing the Count and Recalculating the One Time Password.

Claim 2 recites, in relevant part:

> A method for authenticating a request for access to a resource, comprising:
>
> if the calculated One Time Password does not correspond to the received One Time Password, then incrementing the value of the count at the authentication server and recalculating the One Time Password based upon the incremented count and the secret, and comparing the recalculated One Time Password with the received One Time Password;

Independent claim 6 recites similar features. The Office Action admits that, "Newcombe does not explicitly teach incrementing the count and recalculating." Office Action, p. 5. However, the Office Action asserts that, "Newcombe teaches a window of acceptable values for time with which recalculation can occur and authenticate the client." *Id.* The Office Action alleges that a predictable result of the combination of Matyas and Newcombe is to, "substitute the count value for the time value, perform the incrementing of the count and recalculate to determine if the count was acceptable." *Id.* Applicants respectfully disagree.

The window of acceptable values for a timestamp in Newcombe is not a window within which recalculation can occur as the Office Action alleges. Newcombe discloses a method where the timestamp is extracted from a modified authenticator (the modified authenticator is encoded by the User and is a combination of the local and remote IP addresses and the timestamp). Newcombe, Fig. 8; Fig. 9; [0057]; [0059]. The server then determines if the

timestamp falls within a predetermined range - if it does, the user is authenticated; if it does not, the user is not authenticated. *Id.* at [0092]; [0097]. Notably, there is no recalculation of the modified authenticator or any other calculation if the timestamp falls outside the range. Thus, even assuming, *in arguendo*, that a count could be substituted into Newcombe for the timestamp, the count would simply be extracted from the modified authenticator and then checked to see if it was within a range of count values stored on the server.

The proposed modification of Newcombe by the count in Matyas does not disclose that if the calculated One Time Password does not correspond to the received One Time Password, then incrementing the count and recalculating the One Time Password. Therefore, the Office Action fails to establish a *prima facie* case of obviousness and the rejection of claims 2 and 6 should be withdrawn. The rejection of dependent claims 3-5 and 7-9 is similarly unsupported by the Office Action, and these claims are allowable for at least the same reasons as the independent claims. For at least this reason, it is respectfully requested that the rejection of claims 2-9 be withdrawn.

The Office Action Fails to Show that the Cited References Disclose or Suggest Retrieving the Value of a Count that Corresponds to a Token Based Upon a Serial Number or a User Name.

Claim 2 recites, in relevant part:

> A method for authenticating a request for access to a resource, comprising:
>
> retrieving by the authentication server the value of a count that corresponds to the token based upon the serial number;
>
> calculating by the authentication server the value of a One Time Password based upon retrieved values of the count and the secret corresponding to the token;

Claim 6 recites similar features. The Office Action alleges that, "Matyas discloses retrieving a count." Office Action, p. 5, 6. However, the Office Action fails to show where Matyas discloses that the value of the count that is retrieved corresponds to a token based upon a serial number. Similarly, the Office Action fails to show that Matyas discloses retrieving the value of a count that corresponds to a token based upon a username as recited in Claim 6.

There does not seem to be any disclosure in either reference that could be reasonably interpreted to cover these claim features. Indeed, the section of Matyas relied on by the Office Action to make this rejection merely describes various key-specific information:

> Key-specific information 202 comprises information that changes for each invocation of hash function 430. As shown in FIG. 3, this information 202 may comprise an algorithm ID 206, which identifies the cryptographic algorithm in which the generated keys are used, together with the count 420. (For simplicity, only the count is shown in FIG. 4.) Count 420 is incremented for each successive hash with the same input values Zl and Z2, and is reset whenever Zl or Z2 or the algorithm ID changes. The optional other information 204 may include public information contributed by the parties 102 and 104, public information mutually known to both parties, mutually known private information (such as an authentication key communicated over a separate channel or Zl ‖ Z2), or the like.

Matyas, Col. 5, lines 46-59. There is simply no suggestion in this disclosure that the count value corresponds to a token based on a serial number or a user name. Furthermore, the Office Action admits that, "Matyas does not explicitly disclose a token." Office Action, p.4. It is therefore unreasonable to suggest that the count retrieved corresponds to a token that is admittedly never disclosed in Matyas.

Thus, the Office Action fails to establish a prima facie case of obviousness with regards to claims 2 and 6. The rejection of dependent claims 3-5 and 7-9 is similarly unsupported by the Office Action, and these claims are allowable for at least the same reasons as the independent claims. For at least this reason, Applicants respectfully request that the rejection of claims 2-9 be withdrawn.

A Subsequent Office Action Should not be Made Final.

Claim 1 recites calculating a hash based upon the concatenated secret and count; and truncating the result of the hash to obtain a One Time Password. Claims 2 and 6 recite retrieving the value of a count that corresponds to the token based upon the serial number and upon a username, respectively. These features were presented in claims 1, 2 and 6 as originally filed, and the present Amendment leaves these features unchanged.

The Office Action does not show where these features are described or suggested by the cited art, and does not otherwise provide an analysis to indicate why they would be obvious to one of skill in the art. Therefore, any subsequent rejection of these claims that addresses these features will necessarily include a new ground of rejection that is not necessitated by amendment of the claims or information in an IDS submitted during the period set in 37 C.F.R. §1.97(c). Such an Office Action cannot properly be made final, even if it includes other grounds of rejection that are necessitated by an amendment. *See* M.P.E.P. §706.07(a). It is also respectfully noted that any new position or rationale in a rejection constitutes a new ground of rejection, including: reliance on a new portion of a reference, presentation of a new reference, a new factual finding, application of a new supporting position or rationale, and presenting a new claim interpretation. *See, e.g., In re Kumar*, 418 F.3d 1361, 76 USPQ2d 1048 (Fed. Cir. 2005); *In re Kronig*, 539 F.2d 1300, 190 USPQ 425 (CCPA 1976).

Examiner Interview Requested

As discussed during the February 10 interview, Applicants respectfully request an interview to discuss the amendments and arguments presented herein at the Examiner's convenience, prior to the Examiner taking further action in this case. Applicants' representative can be reached at the number listed below to establish an appropriate date and time.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment in connection with this paper to Deposit Account No. 20-1430.

The undersigned can be reached at 202-481-9900 at the examiner's convenience to set up a follow-up interview in light of this amendment.

Respectfully submitted,

/ASKamlay/
Aaron Kamlay
Reg. No. 58,813

DATE: February 16, 2010

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 202-481-9900
Fax: 415-576-0300
62288301 v1